

Remarks

Claims 1-14, 16-17, 19-30 and 35-38 remain in this application. Claims 15, 18 and 34 were previously canceled without prejudice. Claims 16-17 and 31-33 are hereby canceled without prejudice. Claims 1, 19, 28, 29, 30, 35 and 38 are hereby amended. No new matter is being added.

Claim Rejections -- 35 USC 103

Claims 1-3, 16-17, 19-21, 32-33 and 35-36 were rejected under 35 U.S.C. 103 as being unpatentable over Morley et al. in view of Yoshiura. Claims 4-14, 22-30 and 37-38 were rejected under 35 U.S.C. 103 as being unpatentable over Morley et al. in view of Kowarz. Applicants respectfully traverse these rejections in relation to the claims as now amended.

Claim 1 as amended now recites as follows:

1. A method of securely displaying visual data comprising the steps of:
 - generating a private key and a corresponding public key within a display apparatus;**
 - securely storing the private key within the display apparatus such that the private key is inaccessible from outside the display apparatus;**
 - communicating the public key from the display apparatus to an encryption apparatus;
 - encrypting the visual data at the encryption apparatus using the public key, whereby encrypted visual data is formed;
 - transporting the encrypted visual data from the encryption apparatus to the display apparatus;
 - decrypting the encrypted visual data within the display apparatus such that an electronic version of the visual data is maintained within circuit elements that are substantially inaccessible; and
 - displaying the visual data as a visual image.

(Emphasis added.)

As shown above, the method of claim 1 now requires “**generating a private key and a corresponding public key within a display apparatus**” and “**securely storing the**

private key within the display apparatus such that the private key is inaccessible from outside the display apparatus.” (Emphasis added.)

These limitations are discussed, for example, on page 4, lines 14-19, of the present application, which is reproduced below for convenience of reference.

... Preferably, the display apparatus 26 performs the key production step 30 and the public key output step 32. In this way the private key does not leave the display apparatus 26. Once the public key is available from the public key output step 32, the public key is input to the encryption apparatus 22. Preferably, the display apparatus is designed so that the private key is not accessible from outside the display apparatus 26.

(Emphasis added.)

Applicants respectfully submit that the aforementioned claim limitations of “generating a private key and a corresponding public key within a display apparatus” and “securely storing the private key within the display apparatus such that the private key is inaccessible from outside the display apparatus” (emphasis added) are not disclosed or taught by the combination of Morley and Yoshiura.

Regarding Morley, Morley teaches that key needed to decrypt an encrypted program “is transmitted, or otherwise delivered, to the authorized theaters prior to playback of the program.” (Morley, page 22, lines 10-11, emphasis added.) This teaching of Morley is contrary to the aforementioned claim limitations.

Regarding Yoshiura (“Digital Data Authentication Method”), Yoshiura teaches use of public-private key encryption so as to embed digital signatures into decrypted content for purposes of detecting illegal copies. For example, Yoshiura teaches as follows on column 13, lines 29-56.

To generate the digital signature, the signature generating module 215 calculates the 160-bit hash value of the decrypted content using a predetermined one-way hash function and then encrypts the resulting 160-bit hash value using the signature key stored in the storage module 220.

Once the digital signature is generated, the controlling module 212 tells the signature embedding module 216 to embed the digital signature into the decrypted content inseparably according to a predetermined rule (step 503) and stores then the signature-embedded content in the storage module 220. The digital signature is embedded, for example, by the digital watermark technique explained in Description of Related Art.

Now, assume that the purchaser has created an illegal copy of the content which is stored in the storage module 220 and into which the digital signature is embedded (without an appropriate authority to create a copy) and has transferred the created copy to a third party. As explained in Description of Related Art, the purchaser cannot remove the digital signature, which is embedded in the content, for example, in the form of a digital watermark, from the content. That is, the purchaser cannot create a complete but illegal copy which has no digital signature embedded.

When the illegally-copied content in which the digital signature is embedded is seized, the provider system 100 performs the following to identify the purchaser who created the illegal copy.

Hence, Yoshiura applies public-private key encryption to mark content so as to detect illegal copies. However, there is no disclosure or teaching in Yoshiura in regards to public-private key encryption for the claimed “**method of securely displaying visual data**,” as used, for example, to provide encrypted cinema to movie theaters.

Regarding Kowarz et al., Kowarz et al. is cited in relation to a “grating light valve” aspect. Kowarz et al. does not disclose or suggest the above-discussed limitations relating to the novel application of public-private key encryption to securely display visual data.

Therefore, for at least the above-discussed reasons, applicants respectfully submit that claim 1, as amended, now overcomes its rejection.

Claims 2-14 depend from claim 1. Hence, claims 2-14 overcome their rejections for at least the same reasons as discussed above for claim 1.

Claim 19 is amended similarly to claim 1. Claim 19 now recites “the private key being generated within and securely residing within the display apparatus so as to be inaccessible from outside the display apparatus.” Therefore, for similar reasons

discussed above in relation to claim 1, applicants respectfully submit that claim 19 also overcomes its rejection.

Claims 20-30 depend from claim 19. Hence, claims 20-30 also overcome their rejections for at least the same reasons as discussed above for claim 19.

Claim 35 is amended similarly to claim 1. Claim 35 now recites “the private key is generated within and securely resides within the display apparatus such that the private key is inaccessible from outside the display apparatus.” Therefore, for similar reasons discussed above in relation to claim 1, applicants respectfully submit that claim 35 also overcomes its rejection.

Claims 36-37 depend from claim 35. Hence, claims 36-37 also overcome their rejections for at least the same reasons as discussed above for claim 35.

Claim 38 is amended similarly to claim 1. Claim 38 now recites “the private key is generated within and securely resides within the display apparatus such that the private key is inaccessible from outside the display apparatus.” Therefore, for similar reasons discussed above in relation to claim 1, applicants respectfully submit that claim 38 also overcomes its rejection.

Conclusion

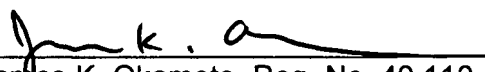
For at least the above-discussed reasons, applicants believe that the pending claims, as hereby amended, are now patentably distinguished over the cited art and are now in suitable form for allowance. Favorable action is respectfully requested.

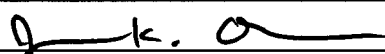
The examiner is also invited to call the below-referenced attorney to discuss this case.

Respectfully Submitted,

Robert W. Corrigan et al.

Dated: April 30, 2007


 James K. Okamoto, Reg. No. 40,110
 Tel: (408) 436-2111
 Fax: (408) 436-2114

CERTIFICATE OF MAILING			
<small>I hereby certify that this correspondence, including the enclosures identified herein, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.</small>			
Signature:			
Typed or Printed Name:	James K. Okamoto	Dated:	April 30, 2007
Express Mail Mailing Number (optional):			